

PATENT APPLICATION
DOCKET NO. PRIT01-00001IN THE CLAIMS

This listing of claims replaces all prior versions and listings of claims in the application.

Listing of Claims

1. (Currently Amended) An apparatus for protecting a computer system, comprising:

a password controller coupled to said the computer system, said password controller capable of receiving being adapted to receive a password attempt transmitted from a user device over a network, and capable of operating being adapted to operate a computer program to compare said the password attempt with a stored password, wherein said the stored password comprises a password segment, and said the password segment comprises:

an entry event comprising [[a]] at least one predetermined entry signal;

a predetermined time interval following said the entry event; and

a terminating signal following said the predetermined time interval, said terminating signal marking the end of said the password segment;

wherein said computer program is capable of allowing the password controller allows the user device to access to said the computer system when the computer program determines that a password segment of said the password attempt matches said the password segment of said the stored password.

2. (Currently Amended) The apparatus as set forth in Claim 1, wherein said computer program is capable of comparing compares a time envelope of said the stored password with a time envelope of a received password attempt, and capable of denying

**PATENT APPLICATION
DOCKET NO. PRIT01-00001**

denies access to said the computer system when said the time envelope of said the received password attempt does not match said the time envelope of said the stored password.

3. (Currently Amended) The apparatus as set forth in Claim 1 wherein said computer program compares said the stored password with said the password attempt received from an online connection to determine whether said the password attempt from said the online connection matches said the stored password.

4. (Original) The apparatus as set forth in Claim 1 wherein said entry event comprises a predetermined combination of computer readable entry signals, wherein each computer readable entry signal comprises one of: a character, a symbol, and a number.

5. (Currently Amended) The apparatus as set forth in Claim 1 wherein said terminating signal is an entry event that follows said the predetermined time interval.

6. (Currently Amended) The apparatus as set forth in Claim 3 wherein said computer program is capable of sending a signal to said the online connection that indicates whether said the password attempt received from said the online connection matches said the stored password.

7. (Currently Amended) The apparatus as set forth in Claim 6 wherein said computer program is capable of waiting until a time delay period expires before sending said the signal that indicates whether said the password attempt received from said the online connection matches said the stored password.

**PATENT APPLICATION
DOCKET NO. PRIT01-00001**

8. (Original) The apparatus as set forth in Claim 7 wherein said time delay period is of variable duration.

9. (Currently Amended) The apparatus as set forth in Claim 1 wherein said stored password comprises at least one password segment comprising a predetermined time interval calculated by subtracting from the total time measured from the trailing edge of a first entry event to the trailing edge of a next second entry event the time required to read said the next second entry event.

10. (Currently Amended) The apparatus as set forth in Claim 2 wherein said stored password further comprises a plurality of password segments wherein the total time of said the plurality of password segments equals said the time envelope of said the stored password, within a predetermined deviation.

11. (Currently Amended) An apparatus for protecting a computer system, comprising:

a password controller coupled to said the computer system, said password controller capable of comprising:

means for receiving over a network, a password attempt generated by a user device; and

capable of operating a computer program to compare for comparing a time envelope of [[a]] the received password attempt with a time envelope of a stored password, and capable of for denying access to said the computer system by the user device when said the time envelope of said the received password attempt does not match said the time envelope of said the stored password.

**PATENT APPLICATION
DOCKET NO. PRIT01-00001**

12. (Currently Amended) A method of protecting [[an]] a computer system, comprising the steps of:

detecting an initial entry event of a password attempt sent over a network by a user device;

determining whether a password segment of said the password attempt matches a password segment of a stored password, wherein said the password segment comprises:

an entry event comprising a predetermined entry signal;

a predetermined time interval following said the entry event; and

a terminating signal following said the predetermined time interval, said terminating signal marking the end of said the password segment; and

allowing the user device to access to said the computer system when said the password segment of said the password attempt matches said the password segment of said the stored password.

13. (Currently Amended) The method as set forth in Claim 12 further comprising the steps of:

calculating a time interval of said the password segment of said the password attempt by subtracting the time required to read a next second entry event from the total time measured from the trailing edge of a first entry event to the trailing edge of said the next second entry event; and

determining whether said the time interval of said the password segment of said the password attempt matches a time interval of said the password segment of said the stored password.

14. (Currently Amended) The method as set forth in Claim 13 further comprising the steps of:

**PATENT APPLICATION
DOCKET NO. PRIT01-00001**

waiting for a time delay period to expire after determining whether said the password attempt matches said the stored password; and

sending a signal that indicates whether said the password attempt matches said the stored password.

15. (Original) The method as set forth in Claim 14 wherein said time delay period is of variable duration.

16. (Currently Amended) The method as set forth in Claim 13 further comprising the step of: determining whether said the entry event of each said password segment of said the password attempt matches a corresponding entry event of said the password segment of said the stored password.

17. (Currently Amended) The method as set forth in Claim 13 further comprising the step of: determining whether said the time interval of said the password segment of said the password attempt matches a corresponding time interval of each said password segment of said the stored password.

18. (Currently Amended) The method as set forth in Claim 12 further comprising the step of: comparing each entry signal in said the entry event in said the password segment of said the password attempt with a corresponding entry signal in said the entry event of said the password segment of said the stored password.

19. (Currently Amended) The method as set forth in Claim 12 further comprising the step steps of:

beginning the timing of said the password segment of said the password attempt at the trailing edge of one of a first entry event and first entry signal; and

**PATENT APPLICATION
DOCKET NO. PRIT01-00001**

concluding the timing of said the password segment of said the password attempt at the trailing edge of one of a next second entry event and next second entry signal.

20-21. (Canceled)

22. (Currently Amended) For use in a computer, computer executable process steps stored on a computer readable storage medium capable of protecting said the computer, comprising the steps of:

detecting an initial entry event of a password attempt sent over a network by a user device;

determining whether a password segment of said the password attempt matches a password segment of a stored password, wherein said the password segment comprises:

an entry event comprising a predetermined entry signal;

a predetermined time interval following said the entry event; and

a terminating signal following said the predetermined time interval, said terminating signal marking the end of said the password segment; and

allowing the user device to access to said the computer system when said the password segment of said the password attempt matches said the password segment of said the stored password.

23. (Currently Amended) The computer executable process steps stored on a computer readable storage medium, as set forth in Claim 22, further comprising the steps of:

calculating a time interval of said the password segment of said the password attempt by subtracting the time required to read a next second entry event from the total time measured from the trailing edge of a first entry event to the trailing edge of said the next second entry event; and

**PATENT APPLICATION
DOCKET NO. PRIT01-00001**

determining whether said the time interval of said the password segment of said the password attempt matches a time interval of said the password segment of said the stored password.

24. (Currently Amended) The computer executable process steps stored on a computer readable storage medium, as set forth in claim 22, further comprising the steps of:

waiting for a time delay period to expire after determining whether said the password attempt matches said the stored password; and

sending a signal that indicates whether said the password attempt matches said the stored password.

25. (Currently Amended) The computer executable process steps stored on a computer readable storage medium, as set forth in Claim 22, further comprising the step of: waiting an arbitrary and variable time delay period before sending said the signal that indicates whether said the password attempt signals matches said the stored password.

26. (Currently Amended) The computer executable process steps stored on a computer readable storage medium, as set forth in Claim 22, further comprising the step of: determining whether said the entry event of each said password segment of said the password attempt matches a corresponding entry event of said the password segment of said the stored password.

27. (Currently Amended) The computer executable process steps stored on a computer readable storage medium, as set forth in Claim 22, further comprising the step of: determining whether said the time interval of said the password segment of said the password attempt matches a corresponding time interval of each said password segment

PATENT APPLICATION
DOCKET NO. PRIT01-00001

of said the stored password.

28. (Currently Amended) The computer executable process steps stored on a computer readable storage medium, as set forth in Claim [[21]] 22, further comprising the step of: comparing each entry signal in said the entry event in said the password segment of said the password attempt with a corresponding entry signal in said the entry event of said the password segment of said the stored password.

29. (Currently Amended) The computer executable process steps stored on a computer readable storage medium, as set forth in claim 22, further comprising the step steps of:

beginning the timing of said the password segment of said the password attempt at the trailing edge of one of a first entry event and first entry signal; and

concluding the timing of said the password segment of said the password attempt at the trailing edge of one of a next second entry event and next second entry signal.

30. (Currently Amended) A method of authenticating a user device, said method comprising the steps of:

receiving by an authentication device, a password sent from the user device in a single data burst transmitted after the user enters the complete password, said password comprising a sequence of predefined characters, wherein the user device separates each of said the characters being separated by a predefined time interval from an adjacent character in the sequence;

determining by the authentication device, whether the received characters match the predefined characters;

determining by the authentication device, whether the received time interval between the received characters matches the predefined time interval; and

**PATENT APPLICATION
DOCKET NO. PRIT01-00001**

positively authenticating the user device only if the received characters match the predefined characters, and the received time interval between the received characters matches the predefined time interval.

31. (Previously Presented) The method of claim 30, wherein the predefined time interval between a first pair of characters is different than the predefined time interval between a second pair of characters.

32. (Previously Presented) The method of claim 30, wherein the step of determining whether the received time interval between the received characters matches the predefined time interval includes:

measuring the time interval between the received characters; and
determining whether the measured time interval is within a predefined positive or negative tolerance value of the predefined time interval.

33. (Previously Presented) The method of claim 30, further comprising waiting for an arbitrary time period after the authenticating step is complete before sending an authorization message from the authentication device to the user device.

34. (Currently Amended) The method of claim 30, further comprising, prior to receiving the password from the user device, the step of sending information regarding the predefined time interval from the authentication device to the user device.

35. (Previously Presented) The method of claim 34, wherein the authentication device periodically sends a new time interval to the user device.

36. (Currently Amended) The method of claim 30, wherein the user device [[is]]

**PATENT APPLICATION
DOCKET NO. PRIT01-00001**

includes a magnetic card reader, and the authentication device is a server in a financial authorization network.

37. (Currently Amended) The method of claim 30, wherein the user device [[is]] includes a magnetic card reader, and the authentication device is [[a]] connected to a server in a financial authorization network.

38. (Currently Amended) In a user device, a method of constructing and transmitting a password utilized by an authentication device to authenticate the user device, said method comprising the steps of:

forming receiving from a user, a sequence of predefined characters forming a password; and

separating each of said characters from an adjacent character in the sequence by a predefined time interval;

identifying a predefined time interval for separating each character from an adjacent character in the sequence; and

transmitting the password to the authentication device with each character being separated from the adjacent character in the sequence by the predefined time interval.

39. (Currently Amended) The method of claim 38, wherein the forming step password includes forming a sequence of at least three characters, and wherein the step of identifying a predefined time interval includes identifying a first predefined time interval between a first pair of characters is different than the and a different second predefined time interval between a second pair of characters.

40. (New) The method of claim 38, wherein the step of identifying a predefined time interval includes receiving the predefined time interval from the authentication device.

**PATENT APPLICATION
DOCKET NO. PRIT01-00001**

41. (New) The method of claim 1, wherein the entry event comprises a plurality of sequential entry signals forming a data block, and the time interval follows the data block.